PARKER SMITH & FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

MANUFACTURING
PRACTICE GROUP

NOVEMBER 10, 2020

CYBERCRIMINALS' NEWEST TARGET: MANUFACTURERS AND DISTRIBUTORS

Josh Hedrick | Principal, Vice President, Account Executive

Because manufacturers and distributors don't handle much consumer data (personally identifiable information), and many do not frequently transact credit card payments, there is a common misconception that they don't have a bona fide cyber exposure. Manufacturers face emerging risks due to greater automation, network-controlled production lines, increasing sophistication of hackers, and risks inherited from external connections such as supply chains, trading partners, and service providers. No longer viewed as merely an IT issue, this exposure has been elevated to the board level. Directors and officers can be sued and personally liable for breaching their duties related to a cyber event.

In recent years, cybercriminals have targeted the healthcare industry to access consumer data and the retail industry where credit card transactions were most prevalent and could be breached. As these industries have evolved and put in more sophisticated controls to avoid losses, criminals have started to target the manufacturing and distributing sector, which may not always have the IT infrastructure or controls in place to combat attacks. According to a new report by professional services firm Sikich, manufacturers and distributors are largely neglecting key cybersecurity concerns. Less than 40% of respondents in the firm's *2020 Manufacturing and Distribution Report* said they performed important data-breach prevention activities, such as penetration testing, phishing exercises with employees, and assessments of vendor and supplier data-security measures. Unsurprisingly, manufacturers and distributors have remained vulnerable to breaches; nearly half of survey respondents said their companies had experienced cyber-attacks within the last 12 months.[1]

The integration of technology into the manufacturing processes, sales, and distribution has created a new and substantial risk, as there could be a high incentive to pay a ransom. With the increased use of robotics and technological advances, manufacturers are having difficulty safely integrating legacy systems, and hackers can render systems unable to communicate and halt operations altogether. These intricate manufacturing systems can be complicated to restore, making them attractive to hackers who demand a higher ransom due to the shutdown length. Manufacturers and distributors have seen an increase in the number of attacks and the size of the demands.

According to Chubb's manufacturing client claims during the past three years, the median cyber incident costs (e.g., call center, notification, crisis response, etc.) climbed to nearly $400,000. In 2018, 86% of manufacturing industry incidents reported to Chubb were caused by someone outside the organization.[2]

continued >

WHAT ARE THE PRIMARY EXPOSURES?

Manufacturers and distributors face significant cyber exposure from business interruption and contingent business interruption, and cyber-crime. Many property and casualty policies require physical damage before they pay, and many are starting to expressly exclude cyber exposures in an attempt to reduce the amount of "silent cyber" coverage.

The following are a few of the exposures facing manufacturers and distributors:

Business interruption/systems failure

Many businesses maintain this coverage for losses resulting from fire, natural disasters, etc., under their property programs. Most property policies won't provide coverage for loss of use of your computer system and networks due to data breach, viruses, or other cyber issues that can shut the business down. Many manufacturers and distributing operations are controlled by their networks. This exposure is exacerbated by the fact that systems can be shut down by something other than a network intrusion, such as a faulty or improper computer and network updates.

Contingent business interruption/systems failure

Similar to business interruption, contingent business interruption poses a significant risk to manufacturers or distributors' operations. Should a key supplier become inoperable and unable to deliver goods or services due to a system intrusion or network failure, the manufacturer or distributor could be unable to produce or provide its products and services and incur extra expenses to remain operational. Expenses could include added costs to source alternative goods or services from different providers.

Invoice manipulation

Invoice manipulation is the release or distribution of a fraudulent invoice or payment instruction to a client or vendor resulting from a network breach. The result is an uncollectable receivable from a client or vendor that has paid a fraudster, believing it was a valid invoice. This normally occurs when employee email accounts are compromised, and criminals watch email traffic for a while, so they can mimic styles and then send fraudulent invoices or payment instructions to clients or vendors.

Unique exposures during COVID-19 and the virtual work environment

Cyber carriers working with manufacturers and distributors continue to have concerns that customers are not taking the necessary precautions to protect sensitive data. The rapid evolution to a virtual work environment for those who can accomplish their work from home tends to create a more insecure remote environment, elevating these organizations' risk. According to Erin Burns, VP at InsureTrust, the country's leading cyber insurance broker, many remote workers in these industries do not have two-factor authentication, proper security and protocols in place, technical updates, and training to avoid phishing scams. Hackers have become more sophisticated and target these new remote workers with COVID-19 topic emails and attachments that utilize malware once clicked on.

WHAT CAN I DO TO PROTECT MY ORGANIZATION AND VIRTUAL WORKERS?

Start with simple communication with your vendors and suppliers

We have suggested that our clients add a disclaimer on the top of their invoices requesting that they be contacted by phone through their main phone number for

continued >

notification of updated bank account or routing information. This step helps keep it front and center for AR/AP staff to pick up the phone and confirm that it is not an imposter providing updated bank information.

Engage with your IT department or a consulting firm to do basic training and penetration testing of your system

Most companies can test how educated their employees are by sending out practice phishing emails and then sharing the results with their population if a number of individuals click on the link, which would have allowed a hacker into the system.

Add a stand-alone cyber policy to your risk management program

Think of this as a safety net should the worst-case scenario occur. This will assist with the expenses and monies paid for cyber extortion, unintentional disclosure of personal information, network security breach, IT forensic costs, legal costs, notification and credit monitoring, regulatory fines, data restoration, and lost profit/business interruption.

These policies should also come with crisis consultants like public relations specialists, legal counsel, and IT forensics teams to assist you in the chaos of a breach situation. They may assist with putting together a cyber-incident response plan, basic phishing tests, vulnerability scans, security assessments, and discounts with anti-phishing software vendors.

What are some claims examples?

1 The 2017 malware attack dubbed NotPetya impacted many large and well-known companies, one of them being Mondelez International Inc., the American multinational confectionery, food and beverage company. After the attack damaged its computer systems, operations were impacted, including production at a Cadbury chocolate factory. According to reports, the company experienced a 5% drop in quarterly sales due to shipping and invoicing delays.[3]

2 A ransomware attack impacted a Pacific Northwest distribution business. They paid the initial ransom amount, but the attackers did not relinquish control of their system. Due to the breach, the distributor was unable to fulfill orders on time as the hackers compromised the warehouse management software. The hackers also gained access to the cold storage area and caused product spoilage as the temperature could not be regulated.

The distributor housed their entire inventory in a rented warehouse, but their policy carried building coverage only as required under a triple net lease. The distributor chose to self-insure their stock/inventory as well as any business personal property. The insurance carrier offered electronic data coverage, which would have provided limited coverage for a loss, but the distributor chose not to carry this coverage. Therefore any cyber claim associated with the housed inventory would be denied. A stand-alone cyber/data breach policy or robust cyber endorsement on the commercial package policy would have made the client whole.

3 Crypto Mining

A local manufacturing company experienced a ransomware attack that resulted in encrypting several of their files. After the insured contacted their carrier through its 24/7 incident response hotline, the insurer offered a consultation with an incident response coach and forensic experts from their cyber panel.

continued >

As a result of these discussions, the company chose not to pay the ransom. However, once the forensic firm began working on remediating the ransomware attack, they discovered that the insured was also a crypto mining victim. The hacking group had installed software in the insured's system that was mining Bitcoin.

As a result of the crypto mining, the bad actor secretly mined cryptocurrency at the expense of the company's system. This surreptitious mining operation led to a drain on the insured's processing power, which extended to service degradation. In addition to the forensics firm and incident response coach, the company incurred credit monitoring and notification fees, as personally identifiable information (PII) was compromised in the attack.[4]

In conclusion, manufacturers and distributors have an ever-growing exposure to cyber risks as their day-to-day operations become more automated and tied to digitally managed supply chains. These industries have become increasingly targeted by hackers as protective controls are not always in place. Phishing scams are targeting virtual workers, and hackers are manipulating invoices to revise bank account information. These losses can cause reputational damage, unfilled orders, and serious business interruption financial losses by a direct loss to the organization or by a contingent business interruption cyber event downstream in the supply chain by a supplier.

Even small steps can help mitigate this exposure by engaging with employees to understand the harm resulting from clicking on a link as many workers move into the virtual environment. Your IT staff can test your workforce with sample emails and coach everyone on the typical links that could allow an intruder into the system. Open up a dialog with your AP/AR staff and their counterparts at customers and suppliers. Include a message on invoices to communicate by phone if any banking information is changed. As a safety net, explore the possibility of cyber coverage if this is an area of concern.

References and Resources

1. Manufacturers, distributors neglect key cyber concerns – report, https://www.insurancebusinessmag.com/us/news/cyber/manufacturers-distributors-neglect-key-cyber-concerns--report-228700.aspx
2. Cyber Risks in the Manufacturing Industry, https://www.chubb.com/microsites/_assets/doc/chubb-cyber/17-01-0230-2019_04-ch_043-chubb-cyber-manufacturing-sheet_v2_final.pdf
3. Six reasons the food and beverage industry needs cyber insurance, https://www.foodfocus.co.za/home/whats-hot/Latest-News/Six-reasons-the-food-and-beverage-industry-needs-cyber-insurance
4. What Have We Paid Lately, Cyber Claims Scenarios 1 & 3, https://www.chubb.com/us-en/_assets/doc/2018-06.15-30-01-0071-what-have-we-paid-lately-2q18.pdf